広域情報制御システムにおけるセキュアマルチキャストグループ管理方式

山本秀典† 鮫嶋茂稔† 河野克己† 足達芳昭‡
(株)日立製作所システム開発研究所† (株)日立製作所情報制御システム事業部‡

1. はじめに

電力、鉄道、一般産業等の分野において、従来の情報制御システムは社内の専用ネットワーク等で構築しており、設備制御を行う制御系サブシステムと計画管理業務等を行う情報系サブシステムとを固定的に接続していた。それに対して近年では、多拠点に分散した制御系サブシステムと情報系サブシステムとをＩＰ網を介して広域に連携させて柔軟に情報共有を図ることが求められている。

ここで情報制御システムでは、システムの段階的な構築、また同一データをリアルタイムに配信すること等の要件を満たすためにマルチキャスト通信が用いられることが多い。一方、マルチキャストされるデータは受信者を制限できない。さらにＩＰ網を介することで他のシステムとも容易に接続できるため、通信データの漏洩が発生する。よってデータ漏洩防止のためにデータの暗号化を行い、暗号強度維持のためにノード間で共有する暗号鍵の（定期的及びノード離脱時の）更新が必要となる。しかし従来方式では鍵更新時に全ノードの鍵の同期化を行う期間中はデータ配信の遅延が発生してしまう。

本稿ではデータを共有するノードの組合せに応じたマルチキャストグループと、それぞれに対応する複数の鍵を各ノードが管理し、鍵をそれぞれ自律的に更新することでデータ配信を遅延させずに鍵更新を行う方式を提案する。

2. 従来技術と問題点

マルチキャストグループのメンバであるノードが離脱した場合のセキュリティ維持、または暗号強度維持のために、各ノードの持つ暗号鍵の更新が必要となり、鍵管理サーバから各ノードへの鍵の配布と各ノードにおける鍵の切替が行われる。IETF(The Internet Engineering Task Force)では IPsec を前提とした、鍵配布のプロトコルが標準化されつつある。ただし鍵の配布、切替の期間内はノード間で新旧の鍵が混在するため、送信側と受信側とでの鍵の不一致のために暗号通信が成立しない場合がある。この対策として鍵の更新期間中は通信を停止して鍵の同期を取る方式、または鍵に付加した因果順序情報（通し番号）を参照して、鍵の配布が遅延した場合、データを受信したノードにて新しい鍵が配布され切り替えるまで復号処理の実行を遅らせる方式が提案されている[1]。

これらの従来方式では、鍵を各ノードに配布し、各ノードでの鍵の整合性をとる期間中はデータ配信の停止または遅延が生じる。情報制御システムにおいて通信のリアルタイム性を重視すると、従来方式では鍵更新に伴うデータ配信の停止または遅延によるシステムのダウンタイムの増加が問題となる。この問題を解決するための提案方式を次章にて述べる。

3. セキュアマルチキャストグループ管理方式

3.1. システムアーキテクチャ

図 1 に本提案方式を導入するシステムアーキテクチャの概要を示す。ネットワークを介して接続された鍵管理サーバとノードが存在する。例えば鍵管理サーバは情報系における設備監視サーバ等と兼ねることができ、ノードは制御系における設備制御端末等に該当する。

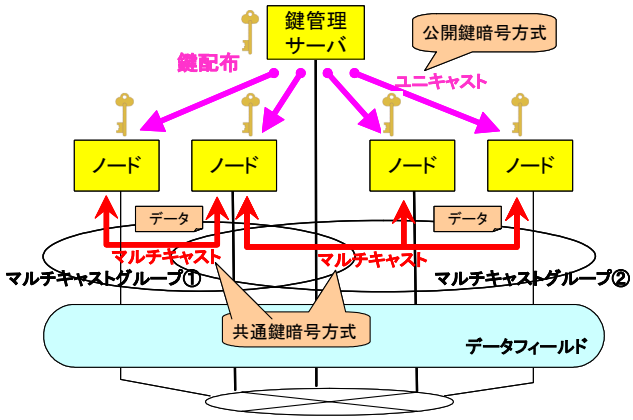

図 1：システムアーキテクチャの概要

マルチキャストグループ毎に暗号鍵を共有することで複数のノードによるセキュアなグルー

Method of Managing Secure Multicast Group for Wide area Information Control System
Hidenori Yamamoto†, Shigetoshi Sameshima†, Katsumi Kawano†, Yoshiaki Adachi‡
Systems Development Laboratory, Hitachi, Ltd.†
Information & Control Systems Division, Hitachi, Ltd.‡

プを形成する。１つのノードは複数のマルチキャストグループに所属することが可能である。このグループ毎の暗号鍵を用いて暗号通信を行うことで、グループ内のみでデータを共有できる。なおこのマルチキャストグループ内の通信に対する暗号化には共通鍵暗号方式を用いる。

鍵管理サーバはグループ毎に暗号化のための共通鍵を作成し、各グループの各メンバノードに鍵を配布する。この時の共通鍵の配布はユニキャストであり、配布する共通鍵は公開鍵暗号方式を用いて暗号化する。なお前述のように鍵管理サーバは定期的及びノードの離脱時に、新しい鍵を作成し、各グループの各メンバのノードに配布するものとする。

3.2. 暗号鍵更新の方式

前章で述べた問題を解決するために本提案方式では、鍵更新時に各ノードにおいて新しい鍵の獲得後も古い鍵を直ちに廃棄することなく、同時に新旧複数のバージョンの鍵を保持しておき、受信データに応じて鍵の使い分けを行う。つまり各ノードにて受信データのヘッダから暗号化に使用された鍵のバージョン情報を参照して、受信側にて該当するバージョンの鍵を取り出して受信データの復号化に用いる。（図２）

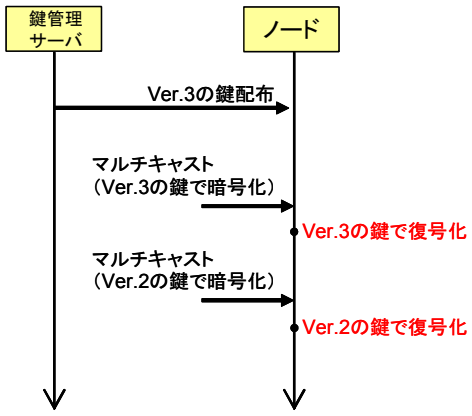

図２：暗号鍵の切替

図３に各ノードにおける鍵格納エリアと共通鍵のバージョン管理の概要を示す。なお鍵格納エリアはマルチキャストグループの鍵毎に確保し、図３では４世代分のバージョンの鍵を保持している。ここで鍵格納エリアはサイクリックに使用し、新しい鍵が配布されたタイミングで、バージョン番号が一番古い鍵から廃棄していく。

なお各ノードにて鍵の現在使用のバージョン（暗号化に用いる鍵のバージョン）は鍵管理サーバからの切替指示を受信した際に新しいバージョンへと更新する。また鍵管理サーバは、鍵の定期配布の場合、鍵を配布してから半周期後に切替指示をブロードキャストにて送信する。

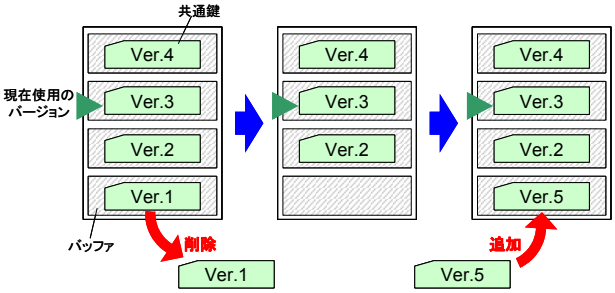

図３：鍵のバージョン管理

3.3. グループ管理

鍵管理サーバは各ノードから定期的に送られる生存信号を参照することでマルチキャストグループのメンバの生存状態を監視する。なお生存信号にはノードを識別する ID、生存状態等の情報が含まれる。

また鍵管理サーバはノードからの生存信号に基づき、メンバのノードの新規加入、離脱時のグループの更新を行う。ノードが新規加入する場合、認証を行い、加入グループの鍵をノードに配布する。ここで情報制御システムでは、メンテナンス等のためにノードが一時的に離脱する場合が多い。このためノード離脱の度に毎回鍵を更新しなくても良い。

ただしセキュリティを強化する場合はノード離脱時も鍵更新を行う。ここでマルチキャストグループにおいて各ノードに自ノード以外のメンバノードの各々に対応する鍵を配布することで、メンバの各ノードがそれぞれ１つだけ加入していないサブグループを形成する。マルチキャストグループよりノードが離脱する場合、鍵管理サーバから生存する残りのメンバのノードに新しい鍵が配布されるまでの期間中、離脱するノードが属さないサブグループの鍵を一時的に用いて暗号化してデータを送信する。これにより離脱したノードのデータ受信を直ちに拒否することができる。

4. おわりに

広域情報制御システムにおけるマルチキャスト通信の効率を保ちつつ、通信データのセキュリティも保証するための鍵更新方式を提案した。

参考文献

[1]“WIDE プロジェクト研究報告書 1999 年度”，WIDE プロジェクト，2000